REMARKS

Upon entry of this Amendment, claims 1-16 are all the claims pending in the application, with claims 1, 6, 11 and 16-19 being in independent form. By the present Amendment, claims 1-16 are amended, and new claims 17-19 are added. No new matter is presented.

Initially, Applicant notes that the Examiner has not indicated acceptance of the drawings filed August 31, 2000. In addition, Applicant notes that the Examiner has not acknowledged the claim to priority from Japanese Application No. 2000-269460. Thus, the Examiner is respectfully requested to indicate acceptance of the drawings and to acknowledge the priority claim in the next action.

In the Office Action, the Examiner rejected claims 1-16 under 35 U.S.C. 102(e) as allegedly being anticipated by Lotspiech et al. (U.S. Patent No. 6,118,873, hereinafter "Lotspiech"). This ground of rejection is traversed

Independent claim 1, 6, 11 and 16 define a novel system and method for decrypting an encrypted computer program presenting new features. For instance, a first cipher key is generated from at least one first block of the encrypted computer program and a first decryption is performed on a plurality of second blocks with the first cipher key. (Specification at page 5, line 13 - page 6, line 21). Further, a second decryption is performed on the plurality of second blocks, wherein for each of the plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. (Specification at page 4, lines 10-21 and page 7, lines 13-20). Thus, the system and method defined by these claims provides for two layers of encryption. Further, in the second layer of encryption, the cipher key is generated for each block from the preceding block which was decrypted prior to the current block.

Notwithstanding the Examiner's rejection, Applicant submits that the limitations of independent claims 1, 6, 11 and 16 is neither anticipated nor suggested by Lotspiech. For example, Lotspiech teaches a system for encrypting television broadcast signals wherein a session key block generator encrypts plural session numbers with a set of device keys which are used by a receiving device, such as set-top box, to decrypt a television broadcast. (Lotspiech at col. 4, line 45 - col. 5, line 20). Upon receiving a set of device keys, an authorized device uses the device keys to decrypt a session number, which is then used to decrypt a television program. (Lotspiech at col. 5, line 42 - col. 6, line 41). Conversely, an unauthorized device is sent a session key block which includes dummy numbers, thereby preventing unauthorized receiving devices from viewing the program. (Lotspiech at col. 6, line 42 - col. 7, line 24).

However, Lotspiech fails to provide any teaching or suggestion for decrypting blocks of a computer program where a first and second decryption of the blocks is performed. Further, Lotspiech suggests nothing about generating a first cipher key from at least one block of a computer program and decrypting a plurality of second blocks of the computer program with the first cipher key. Moreover, Lotspiech suggests nothing about decrypting the plurality of second blocks wherein a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. Indeed, Lotspiech merely teaches the encryption of session key numbers which are broadcast to television receiving devices.

Accordingly, Applicant submits that Lotspiech fails to anticipate or suggest the limitations of independent claims 1, 6, 11 and 16. Accordingly, reconsideration and withdrawal of the rejection of these claims is requested. Further, Applicant submits that dependent claims 2-5, 7-10, and 12-15 are allowable at least by virtue of their respective dependency from independent claims 1, 6 and 11. Thus, withdrawal of the rejection of these claims is requested as well.

For additional claim coverage merited by the scope of the invention, Applicant is adding new claims 17-19. For instance, new claim 17 defines a system for decrypting an encrypted computer program comprising, *inter alia*, means for generating cipher keys for a plurality of blocks, and means for performing a decryption of the plurality of blocks, wherein a cipher key is generated from a current block and a next block is decrypted with the cipher key. Similarly, new claims 18 and 19 defines a method and a computer program product which performs a method, wherein the method comprises, *inter alia*, performing a decryption of a plurality of blocks, wherein a cipher key is generated from a current block and a next block is decrypted with the cipher key. Applicant submits that the limitations of claims 17-19 are neither anticipated nor suggested by the cited art *at least* because Lotspiech fails to provide any teaching or suggestion for decrypting a plurality of blocks wherein the cipher key that is generated from a current block is used to decrypt a next block, as claimed. As discussed above, Lotspiech merely teaches encryption of session key numbers which are broadcast to television receiving devices. Therefore, allowance of new claims 17-19 is respectfully requested.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Brian K. Shelton
Registration No. 50,245

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: June 7, 2005